

Managing Norman Network Protection with Norman Endpoint Manager

Centralized management of the Norman Network Protection (NNP) is performed by the Norman Endpoint Manager, a powerful web based graphical security operations center.

With the dynamic security level indicator and the current status window, the administrator gets instant security state of the network. The management console instantly reports the status of the gateways and malware situation in the environment where one or more NNP's are configured.

The Norman Endpoint Manager provides a central configuration database for multiple NNP's, and keeps the desired configuration and security level through policies. This enables IT administrators to easily manage several NNP's security state remotely making use of policy templates which are fully configurable to keep control of the networks' security state and receive outbreak alerts from any point in the infrastructure.



The management console instantly reports the status of the gateways and malware situation.

IT administrators can easily manage several NNP's security state remotely.

Norman Network Protection

Administering NNP's can be performed using Norman Endpoint Manager or directly at the local NNP admin console. On the local NNP admin user interface you get real time statistics and reports, presenting detected and blocked malware, system statistics and network statistics. This real-time information includes source end destination, address fields, protocols used for transport and detected malware signature or class. The incident log shows currently blocked URL's where malware has been detected.

Setting up NNP to be centrally managed by Norman Endpoint Manager which will extend the management capabilities of multiple NNP's in the network.

You can easily set up any NNP to be centrally managed by Norman Endpoint Manager, which will extend the management capabilities of multiple NNP's in the network.

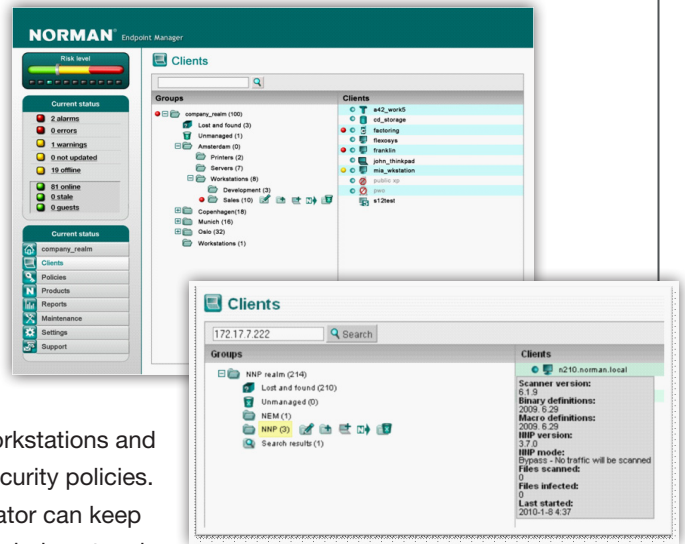
Date	Address	Virus
<input type="checkbox"/> 2007-05-31 13:32:12	cifs://192.168.1.22/Admin/kjlesse.exe	W32/Pebcac.DUHMmm
<input type="checkbox"/> 2007-05-31 13:31:15	cifs://192.168.1.224/Admin/kjlesse.exe	W32/Pebcac.DUHMmm
<input type="checkbox"/> 2007-05-31 13:31:21	cifs://192.168.1.128/Admin/kjlesse.exe	W32/Pebcac.DUHMmm
<input type="checkbox"/> 2007-05-31 13:30:43	cifs://192.168.1.34/Admin/kjlesse.exe	W32/Pebcac.DUHMmm
<input type="checkbox"/> 2007-05-31 13:32:37	cifs://192.168.2.176/Swdlat/portimage.exe	W32/Payload.DD
<input type="checkbox"/> 2007-05-31 13:31:29	cifs://192.168.2.221/Swdlat/portimage.exe	W32/Payload.DC
<input type="checkbox"/> 2007-05-31 13:31:33	cifs://192.168.4.8/Shared/Greetingcard.exe	W32/Troj_JHY

KEY FEATURES

- Provides current status window for instant information about the security state of the network
- Provides overview of all network devices and status on all Norman clients*
- Generates and displays event and status statistics
 - Manages incoming alarms, warnings and errors
- Manages configurations for current and future products
- Manages policies and assigns them to clients & nodes
- Manages product installation in a network
- Manages Internet Update policy
 - Backup for configuration and database
 - Serves as a distribution point for definition files and software updates

Norman Endpoint Manager

Norman Endpoint Manager (NEM) is a web based graphical application designed for managing Norman anti-malware products. The NEM features a unique passive discovery technology detecting all IP based devices in the network, which gives the network administrator the complete overview of all devices attached to the network. With NEM, the IT administrator can deploy Norman Endpoint Protection clients to laptops, workstations and servers*, and manage them all through security policies. With the built-in policy tool, the administrator can keep the desired security state throughout the whole network.



Managing the NNP is an easy task as malware alerts, status information, warnings and errors are located in the console. A mouse-over function gives vital information about the unit, scanner engine and malware situation.

Security Policy based management

The powerful Policy Engine makes it easy to deploy policy settings throughout the infrastructure. The policies let the administrator keep the desired security state in groups of workstations, desktops, servers, Exchange servers and NNP's at all times. The policy tool makes use of policy templates which are fully configurable, and contains dedicated policy templates for the different product groups.

Security health status at a glance

Norman Endpoint Manager provides a dynamic security level indicator and a current status window, giving the IT administrator instant information about the security state of the network. Malware incidents, outdated clients/gateways or system warnings will affect the indicator and report detailed incident information through status views, messaging and alarm modules.

The system allows for integration with other management tools as an advanced Message Handling System (MHS) takes care of sending alerts and incidents to other management systems via email, SNMP, SMS, Syslog or Eventlog.

The risk level bar and status view module present the network's security health status at a glance. Adjustment and tuning capabilities enables the administrator to trigger important and necessary warnings and alarms.



Network security status is reflected in the dynamic Risk level indicator.

*Requires Norman Endpoint Protection license.



Norman ASA is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor. While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services. Norman was established in 1984 and is headquartered in Norway with continental Europe, UK and US as its main markets.

www.norman.com

Norman SandBox® US Patent Number 7,356,736

NORMAN®